IN THE CLAIMS

Pending claims follow:

1. (Currently Amended) In an environment that includes a plurality of users , wherein each user possesses secrets that are shared by respective sets of said plurality of users, a secret updating method, comprising:

(a) updating at least one compromised secret known by at least one evicted user using at least one non-compromised secret that is not known by said at least one evicted user;

wherein said updating does not use new secret information.

2. (Original) The method of claim 1, wherein said updating comprises updating a plurality of compromised secrets.

3. (Original) The method of claim 1, wherein said updating comprises updating all compromised secrets.

4. (Original) The method of claim 1, wherein said updating comprises updating at least one compromised secret known by one evicted user.

5. (Original) The method of claim 4, wherein said updating occurs upon an eviction event.

6. (Original) The method of claim 1, wherein said updating comprises updating at least one compromised secret known by a plurality of evicted users.

7. (Original) The method of claim 6, wherein said updating occurs on a periodic basis.

8. (Original) The method of claim 1, wherein said updating comprises updating a compromised secret using one non-compromised secret.

9. (Original) The method of claim 1, wherein said updating comprises updating a compromised secret known by a set of users using a non-compromised secret of a subgroup of said set of users.

10. (Cancelled)

11. (Original) The method of claim 1, wherein said compromised secret is shared by said plurality of users.

12. (Original) The method of claim 1, wherein said secrets enables secure communication.

13. (Currently Amended) In an environment that includes a plurality of users , wherein a first user possesses a set of keys, said set of keys including a first key that enables secure communication among a set of users, said set of users including at least said first user and a second user, a keying method, comprising:

(a) upon eviction of at least said second user, determining an updated first key using information that includes said first key and a second key, wherein said second key enables secure communication among a subgroup of said set of users, wherein said subgroup does not include users subject to said eviction;

wherein said determining uses a function having the following properties: (1) knowledge of said updated first key does not give knowledge of said first key or said second key, (2) knowledge of said first key does not give any knowledge of said updated first key, and (3) knowledge of said first key and said updated first key does not give any knowledge of said second key.

14. (Original) The method of claim 13, wherein only said second user is evicted.

15. (Original) The method of claim 13, wherein said second user and one or more other users in said set of users are evicted.

16. (Cancelled)

17. (Currently Amended) The method of claim [16]13, wherein said determining uses a one-way function.

18. (Original) The method of claim 17, wherein said updated first key is equal to F(first key, second key), wherein F() is a one-way function.

19. (Original) The method of claim 13, wherein said determining uses only said first key and said second key.

20. (Original) The method of claim 13, wherein said subgroup includes only said first user.

21. (Original) The method of claim 13, wherein said subgroup includes a plurality of users.

22.-27. (Cancelled)

28. (Currently Amended) A keying method in an environment having a plurality of users , each user being capable of storing a set of keys that enable secure communication among sets of said plurality of users, comprising:

(a) distributing first information that enables users to update, after eviction of one or more users, a set of compromised keys that are known to said one or more users without receiving new key information;

wherein said update does not include new secret information.

29. (Original) The method of claim 28, wherein said first information includes information that enables identification of a one-way function.

30. (Original) The method of claim 28, wherein said first information includes information that enables identification of said evicted one or more users.

31.-37. (Cancelled)

38. (Currently Amended) A secret sharing system, comprising:

a key server that distributes secret information to a plurality of users, wherein each user is sent secrets that are shared by respective sets of said plurality of users, said key server being operative to update at least one compromised secret known by at least one evicted user using at least one non-compromised secret that is not known by said at least one evicted user;

wherein said update does not include new secret information.

39. (Currently Amended) A computer program product, comprising:

computer-readable program code for causing a computer, in an environment that includes a plurality of users, wherein each user possesses secrets that are shared by respective sets of said plurality of users, to update at least one compromised secret known by at least one evicted user using at least one non-compromised secret that is not known by said at least one evicted user; and

a computer-usable medium configured to store the computer-readable program codes;

wherein said update does not include new secret information.

40. (New) The method of claim 1, wherein said non-compromised secret utilized for said updating is known by all users in said plurality of users and is not known by said at least one evicted user.

41. (New) The method of claim 40, wherein a single non-compromised secret is utilized to update a plurality of compromised secrets by using a one-way function with inputs of said single non-compromised secret and said non-compromised secret.